10/510372

DT04 Rec'd PCT/PTO 05 OCT 2004

or even damage to the system may

occur, and also, depending on the system, the surroundings and the environment may, under certain circumstances, also be put at risk or damaged. EP 617350 therefore proposes to carry out user authentication in the communications device before instruction information is actually input. For this purpose, a password or a code number containing the authorization for access to the communications device and thus to the system must be input.

While the risk of access by unauthorized persons can largely be prevented by user authentication, there is nevertheless a certain residual risk. This is in particular the case if the password or the code number is, or becomes known, to unauthorized persons.

One particular risk is also constituted by what are referred to as hacker attacks. These are attacks by unauthorized persons who aim to guess the password and/or code number through repeated attempts. In particular, systems of this kind whose communications devices have links to computer networks are particularly at risk here as the hacker attacks can be automated using computer programs and/or scripts so that a very large number of attempts at guessing a password and/or code number can be carried out within a short time.

The invention relates to a method for remotely controlling and/or regulating devices according to WO 01/72012. In the disclosed method, a communication with a validation code is transmitted by the system to a receiver by means of a communication device. The validation code can be used by the receiver to provide a message to the system with a check code. In the system, the check code can be extracted from the message and the authenticity of the message checked by

Art 34.

means of the validation code and check code. Since the validation code and check code are used to authenticate messages and are independent of addresses of the receiving devices, when necessary the same validation code and check code can be used for different devices.

WO 01/48722 discloses a remotely controlled telemetry module which is configured as a sensor and control device. If a message is received by the device, control instructions contained in it are to be carried out only if the message has been dispatched by an authorized person. For this purpose, it is checked whether at least part of the call number of the dispatcher corresponds to a stored authorization call number. This requires the communications network to support the transmission of the dispatcher call number. The identification of the dispatcher takes places independently of the message to be transmitted and also cannot be encrypted together with said message or independently of it. This type of dispatcher identification and authorization therefore provides only a certain degree of security.

US Pat. No. 6'201'996 B1 discloses a method and a device for remotely controlling an industrial system by means of the Internet. For the sake of user security, a password-protected access to the web page of the communication device, an encryption of data to be transmitted via the network and a suitable user authentication process, with which the user obtains access to a regulated web page by means of which he can control the system, are disclosed. The identification of the dispatcher is not an integral component of the message to be transmitted to the web page. Instead, the user authentication is again carried out before granting access to the data to be protected or to the check mechanisms and is carried out independently of the data or instruction information to be protected.

EP 0 930 792 discloses a system and a method for the wireless transmission of status data to a device interface. In order to prevent misuse, identification data of the dispatcher can be transmitted with the message. For this purpose, for example the telephone number of the dispatcher of the message is transmitted.

Description of the invention

For this reason, the object of the invention is to specify a method for remotely controlling and regulating systems which effectively minimizes the risk of manipulation by unauthorized persons and in particular protects against hacker attacks.

The object of the invention is also to specify a reliable method for remotely controlling and/or regulating a system which does not require a user authentication to take place before actual transmission of instruction information, so that said method is simple and efficient.

These objects are achieved by means of a method as claimed in claim 1. A communication which comprises information relating to the system and a validation code is dispatched here by a communication device assigned to the system, preferably to a receiver device which is determined in advance. As soon as the communication device receives a message at a time after the communication has been dispatched, a check code is extracted from this message according to a predefined rule. The origin of the message is checked by means of the validation code and check code taking into account the predefined rule, i.e. it is checked whether the message originates from a receiver of the communication. It is thus possible to use the validation code and check code to verify whether the received message constitutes a response to the dispatched communication.

In this context, the validation code has a chronologically limited validity and a validity information is added to the validation code.

Only in cases in which it has been successively checked whether the message originates from a receiver of the communication, an instruction information is both extracted from the received message in addition to the check code according to the predefined rule and processed and/or executed by the systém.

If, on the other hand, it was not possible to use the validation code and check code to verify that the received message constitutes a response to the dispatched communication, either the instruction information is not extracted at all from the message or the extracted instruction information is ignored.

This object and further objects, advantages and features of the invention become clear from the following detailed description of a

Art 34.

device is preferably provided between the communication device 2 and system 1, the instruction information being transmitted to said control device and passed on from it to the system 1. If the checking was not successful, the instruction information is ignored.

The first extraction rule is preferably configured in such a way that the check code and instruction information is extracted by cutting out parts of the message.

As is apparent from the previous explanations, one application of the method according to the invention ensures that only a receiver of the communication, and thus of the validation code, is capable of issuing instructions for remotely controlling and/or regulating the system 1. In order to do this, the receiver must firstly extract the validation code from the communication in accordance with a second extraction rule which constitutes a reversal of the first combination rule. From the instructions which it attempts to issue, it can generate a message together with the validation code given knowledge of the first extraction rule and the communication device 2 extracts a check code from this message after it has received it, which check code leads to successful checking of the message and thus to the extraction and implementation of the instruction information. To do this, it must use a second combination rule which ensures this.

In a further preferred configuration of the method according to the invention, dispatcher information is extracted from the message in accordance with a third extraction rule. In the communication device 2, the dispatcher information is checked and the instruction information is passed on from the communication device 2 to the system 1 and/or processed only in the case of successful dispatcher identification, i.e. correspondence between the dispatcher information and stored dispatcher data of authorized users. The dispatcher information preferably contains here a secret password or a secret code number. In this case, the operation is what is referred to as a strong user authentication, i.e. the dispatcher is authenticated as an authorized user by virtue of the fact that, on the one hand, he knows something - namely the password or code number - and, on the other hand, he possesses something - in the present case the receiver device 3 to which the communication was transmitted, or alternatively the communication which he has received with the receiver device 3. Here, the receiver of the communication must add, in accordance with a third combination rule, the dispatcher information to a message which he generates.

In one preferred refinement of the method according to the invention, the validation code, check code and/or dispatcher information are transmitted in encrypted form. To do this, the validation code and/or dispatcher information itself is preferably encrypted before it is added to the communication or message in accordance with a first or third combination rule, respectively.

However, the entire communication and/or message can also advantageously be encrypted. If the communication device 2 receives an encrypted message, it must firstly be decrypted. If the check code or dispatcher information is present in an encrypted form after extraction from the message, it is to be decrypted. If the message contains dispatcher information, the risk of manipulation by unauthorized persons is reduced further by encrypted transmission because the dispatcher information cannot readily be acquired from illegitimately monitored or intercepted messages. Even if the validity of the validation code is to be subject to a chronological limitation, encrypted transmission is advantageous. In this case, validity information can be added directly to the validation code, for example by appending. Manipulation of the validity information by the receiver is ruled out. After decryption of the message or check code in the communication device 2, the validity information is available

PATENT CLAIMS

1. A method for remotely controlling and/or regulating at least one system (1), in particular an industrial system,
   - using a communication device (2) which is assigned to the system (1),
   - wherein a communication is dispatched by the communication device (2),
   - the communication comprises information relating to the system (1) and a validation code, and
   - from a message which the communication device (2) receives after the communication has been dispatched,
     - a check code is extracted according to a first extraction rule and
     - by means of the validation code and the check code it is checked whether the message originates from a receiver of the communication, and
     - only if the checking is successful, an instruction information according to the first extraction rule is extracted from the message and is implemented by the system (1),
   - wherein the validation code has a limited period of validity, characterized in that
   - a validity information is added to the validation code.

2. The method as claimed in claim 1, characterized in that
   - the validity information is appended to or is prefixed to the validation code.

3. The method as claimed in one of the preceding claims, characterized in that
   - the validation code is valid once.

4. The method as claimed in one of the preceding claims, characterized in that

- the validation code is generated by a random number generator.

5. The method as claimed in one of the preceding claims, characterized in that

- the validation code is transmitted in encrypted form.

6. The method as claimed in one of the preceding claims, characterized in that

- the validation code itself is encrypted before it is added in accordance with a first combination rule to the communication or message.

7. The method as claimed in one of the preceding claims, characterized in that

- the check code is transmitted in encrypted form.

8. The method as claimed in one of the preceding claims, characterized in that

- by the receiver of the communication, a dispatcher information is added to the message, which he generates, in accordance with a third combination rule,
- the dispatcher information is extracted from the message in accordance with a third extraction rule,
- by means of the dispatcher information and stored dispatcher data the dispatcher is identified,
- only if the checking, as to whether the message originates from a receiver of the communication, is successful and if the identification of the dispatcher is successful, an instruction information is implemented by the system, after the check code and dispatcher information have been extracted from

the message, and

- if the checking and/or the identification of the dispatcher were/was not successful, the instruction information is ignored.

9. The method as claimed in claim 8, characterized in that

- the dispatcher information contains a secret password or a secret identification number.

10. The method as claimed in either of claims 8 and 9, characterized in that

- the dispatcher information is transmitted in encrypted form.

11. The method as claimed in one of claims 8 to 10, characterized in that

- the dispatcher information itself is encrypted before it is added to the message in accordance with a third combination rule.

12. The method as claimed in one of the preceding claims, characterized in that

- the entire communication and/or message are encrypted.

13. The method as claimed in one of the preceding claims, characterized in that

- the communication and/or the message are dispatched and/or received by means of short message service.

14. The method as claimed in one of the preceding claims, characterized in that the message is received via Internet.